全球政治評論　*Review of Global Politics*

第七十七期（2022）No.77 頁 129-136

書評

加密貨幣的政治與經濟：比特幣、以太坊、穩定幣、臉書幣將如何改變全球金融系統

CRYPTOCURRENCY: How Digital Money Could Transform Finance

李 旭 糖 *Jiu-Tang Li*
國立中興大學國際政治研究所碩士生
M.S. Student of Graduate Institute of International Politics
National Chung Hsing University

一、何為加密貨幣？

「什麼是加密貨幣?」根據歐洲中央銀行（European central bank）2012年發布的虛擬貨幣框架（Virtual Currency Schemes），定義加密貨幣屬於數位貨幣的一種，由開發者發行與管控，供特定虛擬社群成員使用。[1] 到了 2019年歐洲央行再將加密貨幣（或稱加密資產、虛擬貨幣、加密代幣）定義為「一種以數位形式記錄並透過使用加密技術實現的新型資產，不代表對任何可識別實體的財務債權或負債。」表明其特點是缺乏潛在的債權，這使得它們具有高度的波動性和投機性。[2]

---

[1] European Central Bank, "Virtual Currency Schemes," *ECB*, October 2012, *https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf*.

[2] European Central Bank, "Crypto-assets– trends and implications," *ECB*, June 2019, *https://www.ecb.europa.eu/paym/intro/mip-online/2019/html/1906_crypto_assets.en.html*.

而為什麼會有這樣的轉變呢?從本質上來看加密貨幣是一種利用加密技術且不再依賴任何中介者的情況下，[3] 藉由網路交換價值單位的方法。[4] 但就像所有定義都會遇到的問題一樣，答案不只一種，若要了解這個問題必須從加密貨幣的歷史故事說起，加密貨幣最初是源於一項政治計畫，目的在於推出可能破壞「政府」此一概念的技術，也就是無國界的數位現金，追求這一個目標的是一群自稱「密碼龐克」（cypherpunk）的人，他們是數位科技與自由意志主義混合的結晶，認為網路必須成為自由、自主、連結，以及不受限制地共享知識的空間，而政府是威脅這個理想的主因，因為政府設法控管網路、監視用戶，將世界變成一個扼殺自由的全球監獄。1980 年代中期，密碼龐克開始討論，期望加密電子郵件、匿名網路和安全認證系統可以讓用戶在政府眼前隱形、避開監控，資訊和商品將能「真正」自由流通，他們的終極理想是「加密無政府狀態」（crypto-anarchy），[5] 這是一種泯除國界、基於自願（在匿名狀態下）的自由貿易系統，最後的結果會是我們今天所認知的政府形式走入歷史，沒有國界、沒有法律也毋需繳稅。[6] 密碼龐克開始努力找尋發行此種數位貨幣的方法並解決所遇到的難題，但他們一直尚未找出能夠同時達到去中心化、預防網路攻擊與詐騙交易、能既保持對外開放又使參與人願意共同承擔風險、成本也不會太高的平衡點，這個局面直到 2008 年中本聰（Satoshi Nakamoto）發表了一篇名為《比特幣：一種對等式的電子現金系統》（Bitcoin: A Peer-to-Peer Electronic Cash System）的 9 頁文件後有了突破。

二、加密貨幣的發展與轉變:從去中心化到智能合約

[3] 透過加密貨幣，某甲可以任意發送一個價值單位給某乙，無須銀行、支付公司，或任何類型的機構插手，完整的匯款流程由分散的電腦聯合起來確保，其中不管哪一台電腦都無權自行阻止或操控付款。

[4] 吉安·沃爾皮切利，《加密貨幣的政治與經濟》（新北：真文化/遠足文化，2021 年），頁 9。

[5] 此詞源於密碼龐克兼英特爾科學家提摩太·梅伊於 1992 年發布名為《加密無政府主義者宣言》的書冊。

[6] 前揭書，頁 15-16。

2009 年比特幣網絡開始啟動，中本聰透過區塊鏈（Blockchain）與分帳式帳本技術（Distributed ledger technology, DLT）設計出能直接點對點進行交易支付的去中心化系統，並以分散式節點（node）的方式來批准交易。它的出現正值 2008 年金融海嘯爆發過後，當時輿論充斥著許多政府如何對銀行進行緊急救助的計畫，而比特幣則以反對銀行和政府支出的姿態登場，這個時候比特幣譜出的願景是讓貨幣能夠做到沒有支付公司、沒有金融機構、沒有中央銀行，只有數學代碼，這種消除中介層的願景，也是大部分在比特幣之後出現的加密貨幣的重心。雖然去中介化的概念在 1960 年代就有經濟學家提出，以用來描述降低依賴商業銀行和退休基金等中介機構的趨勢，[7] 但隨著網路的興起，這個概念在現今時代得以實現並且成為可能影響到許多產業的現象。

2011 年，維基解密（WikiLeaks）創建人朱利安·保羅·阿桑奇（Julian Paul Assange）被政府列入黑名單無法透過傳統支付平台募集資金後，維基解密開始接受以比特幣募款，同年，暗網上推出非法毒品交易平台「絲路」（Silk Road）並以比特幣作為支付方式，雖然此時實現了加密無政府狀態的理想，但比特幣卻被貼上犯罪貨幣的汙名，許多人因而為其非法用途而躊躇不前，2013 年，絲路在創辦者被逮捕後關閉運作反而推動了比特幣的全球使用量飆升，這也開啟了比特幣作為投機性投資工具的契機，許多投資人鑑於金融危機所帶來資產貶值的風險尋求政府權限外的保值管道，截至今日，全球比特幣總市值約為 1.284 兆美元。[8]

2015 年，維塔利克·布特林（Vitalik Buterin）發明的「以太坊」（Ethereum）為整個加密貨幣的典範開啟新的頁章，原先比特幣的設計在應用上出現了諸多限制，例如區塊可容納的交易量不足但擴充區塊會使經營節點成本變高，限制其處理交易的速度及去中心化的穩健性，交易帳本完全公開的設計使匿

[7] 同前註，頁 36-37。

[8] 林國賓，〈加密幣市值 直逼 3 兆美元〉，《工商時報》，2021 年 11 月 10 日，*https://ctee.com.tw/news/global/545982.html*。

名的安全性因第三方交易平台的出現而有風險，更別說為人詬病的環保問題。[9] 以太坊的設計避免了大量耗材的問題，在以太坊的區塊鏈上除了支援以太幣的轉帳功能外，提出「智能合約」（Smart Contract）的概念，智能合約是利用數位技術建立的財務契約，如果支付一筆款項，或輸入任何訊息到以太坊某個智能合約帳戶，該契約就會自動觸發代碼執行，所有契約內容都會被記錄在電腦代碼中，這意味透過大量不同指令的組合可以設計幾乎所有想像到的合約操作，[10] 而合約的執行無須依賴律師或中間人，也無須擔心契約詐欺、義務不履行的問題，以太坊的創新為我們展現了去中心化的應用不僅適用於支付，還適用於整個金融操作與軟體應用程式，加密貨幣的發展將影響許多與我們生活切身相關的產業，從最基礎的轉帳交易到物權、債權合約、保險契約與賭博事業，甚至是選舉投票的運作方式。

以太坊為我們所建構的最終目標是「去中心化自治組織」（Decentralized Autonomous Organization, DAO），以太坊本質上是一個以經濟交易為主的平台，若說比特幣的問世目的在於扼殺銀行家、支付公司和美聯儲，以太坊的去中心化和中介化選定打擊的對象包括了所有我們看的到的大公司，DAO 要創造的是一個公司無須經理與執行長的時代，創建所有交易不會受到層層剝削、哄抬價格的組織，以及阻絕企業高層暗地裡的詐欺與貪腐行為。[11]說到這裡就足夠振奮人心了，但有趣的是，這個概念既是民粹的也是反民粹的，他們對 Amazon、Uber 和其他的資本主義平台巨獸豎起中指，但對每個都在工作的人來說也是一樣的。這轉變可以發現，以太坊去中心化的目的不再是為

---

[9] 根據劍橋大學替代金融中心（Cambridge Center for Alternative Finance，CCAF）的資料，比特幣目前每年大約消耗 1,100 億度的電，占全球電力產量的 0.55%，大約相當於馬來西亞或瑞典等小國一年的能源用量。

[10] 布特林認為以太坊具圖靈完備（turning complete）的特色，其代表的是以太坊用區塊鏈的方式連接了全球所有的機器，組成一個強大的硬體基礎，在以太坊系統中，設置了虛擬計算程序。以太坊內置了多種程式語言的區塊鏈協議，這些程式語言都是圖靈完備的，可以支持條件分支、循環、跳轉、函數調用等複雜的運算邏輯，理論上可以在以太坊區塊鏈上運行任意的應用。

[11] 同前註，頁 60-62。

了抗拒特定機構，而更像是抗拒任何人所可能進行的任何形式的控制。[12]

三、金融體系的未來與政府的角色?

加密貨幣的演進過程中雖然遇到許多問題，例如 The DAO 事件，[13]和首次代幣發行（Initial Coin Offering, ICO）風潮泡沫化，[14] 許多像布特林一樣致力於建立該理想的工程師們一直以來努力解決設計上的問題來避免災難發生的機率，經歷過加密寒冬（crypto winter）後加密貨幣的發展開始走向穩健、更謹慎的方向，[15] 故有了穩定幣的出現，不過依舊沒有脫離去中心化的核心概念，穩定幣在一路跌跌撞撞的持續修正最後衍生出現今受到熱烈注目的概念，那就是「去中心化金融」（Decentralized Finance, Defi）。

DeFi 相對於傳統中心化的金融服務（CeFi），將金融產品建立在公共的、去中心化的區塊鏈網絡上，透過像是智慧合約的編程協定，DeFi 能發展相同的金融產品，但不同以往的銀行、保險、證券交易等傳統形式需要一個監管中心，Defi 是寫在區塊鏈上的金融服務系統，在這套系統上所有的買家、賣家、甚至貸方、借款人，都能進行點對點、不受中心監管的金融活動。[16] 隨著 DeFi 目前發展中的應用範圍日漸擴大，包含了去中心化交易所、借貸、支付、衍生品、資產管理和保險等透過加密貨幣進行應用的各種金融業務。

---

[12] 同前註，頁 64。

[13] The DAO 事件，The DAO 創投組織就是採用了以太坊技術，來建立一個萬用的智能合約平臺，想要打造出一個分散式自治組織。The DAO 在 2016 年 4 月時啟動「以太幣」募資專案後，在 27 天內就募得 1,200 萬個以太幣。同年 6 月 The DAO 遭駭客攻擊，被盜領了約 370 萬個以太幣。

[14] 首次代幣發行風潮是當時透過銷售無形代幣（Token）資產的方式來籌措資金的風氣，任何有想法的人都可以繞過風險資本家和機構投資者的介入直接向未來用戶籌集資金，檯面上出現許多參差不齊的加密代幣，也引發許多詐騙行為，一度造成混亂。

[15] ICO 的風潮隨著狂熱的交易、欺詐性的銷售，以及監管上的混亂，於 2018 年泡沫化，加密貨幣領域隨即進入加密寒冬階段。創建者們和加密貨幣論壇內部都經歷過許多反思與辯論。

[16] 當金融服務存在著「不需被授權就能進行交易」、「可自行決定金融服務內容或協議（protocol excution）」的特質，被稱為真正的 DeFi 去中心化金融。

這是另一個平行於現有金融系統的新服務，將在現有金融市場引進更多的創新競爭，過去國際金融監理機構對加密貨幣與 DeFi 多抱持保守的態度，[17]但隨著 DeFi 生態不斷擴大，使用者越來越多，根據 Crypto.com Research 最新公布的數據，全球持有加密貨幣的人數，從 2021 年 1 月 1.06 億人增加到的同年 6 月增長到 2.2 億，[18] 雖然從交易數量來看加密貨幣網絡要跟上現存傳統交易平台還有一段距離，[19] 但國際監理機構正在努力改變銀行對加密貨幣的看法，認為這些資產可以積極推動金融機構進入創新和效率的新時代。[20]我們可預見的是 Defi 對於未來全球金融體制將產生巨大的變革與影響。

值得注意的是，不論比特幣、以太坊和穩定幣等如何發展，各國政府對加密貨幣的態度不盡相同，直到 2019 年臉書公布即將推出天秤幣的計畫後，才在政府間引起軒然大波，當科技企業龍頭聯手合作進入加密貨幣領域，[21]最

---

[17] 摩根大通（JP Morgan Chase）的執行長傑米戴蒙（Jamie Dimon）於 2014 年聲稱，加密貨幣是一種「可怕的」價值儲存手段，同時也被用於非法目的，金融業呼籲加強管制，甚至禁用的呼聲時有所聞。到了 2021 年，摩根大通已將 2 家加密貨幣交易所 Coinbase 和 Gemini 納為銀行客戶，紐約金融服務部（NYDFS）也開始為比特幣業務發放許可證，根據 Crypto.com 的報告，目前全球已有 2.2 億人使用加密貨幣。

[18] Sheldon Reback, "Crypto User Numbers Double in 6 Months," *CoinDesk*, July 29, 2021, *https://www.coindesk.com/business/2021/07/29/crypto-user-numbers-double-in-6-months/*.

[19] 比特幣網絡在 2021 年平均每季度處理了 4890 億美元的交易；PayPal 在 2021 年平均每季度處理 3020 億美元的交易；萬事達卡網絡每季度處理 1.8 萬億美元的交易；而 Visa 網絡每季度平均處理 3.2 萬億美元。交易數量對比，比特幣網絡平均每季度處理 2500 萬筆交易，大約每天 28 萬筆交易。而萬事達卡在過去一年中平均每季度處理 330 億筆交易，即每天 3.66 億筆；Visa 平均每季度處理 537 億筆交易，即每天 5.97 億筆。(依據 PayPal、萬事達卡和 Visa 的交易額季度報告，以及 BlockchainCom 美元計算的比特幣交易額)
Sam Wouters, "When might the Bitcoin network process volumes like Mastercard & Visa?," *blockdata*, December 21, 2021, *https://www.blockdata.tech/blog/general/bitcoin-volume-mastercard-visa*.

[20] 蘇偉華，〈從排斥到擁抱，金融業看見 DeFi 新機會〉，《風傳媒》，2021 年 12 月 13 日，*https://www.storm.mg/article/4084939?page=1*。

[21] 該計畫總體控制權掌握在位於日內瓦的非營利組織天秤幣聯盟手中，成員包括科技和金融巨頭，如 Uber、Lyft、Spotify、Coinbase、Paypal、Stripe、Visa 卡、萬事達卡、eBay 等大公司。每個都出資 1000 萬美元為天秤幣提供資金，預期從轉帳費用和儲備金資產的利息中抽取利潤，並在天秤幣網經營一個節點。(該區塊鏈僅有 28 個成員可以經營節點，是否能稱為加密貨幣或是區塊鏈的說法受質疑)

擔心天秤幣的人不是技術專家和密碼龐克，而是政府。

天秤幣的發行目的做為一種私人的全球貨幣，其白皮書洋洋灑灑地說明天秤幣如何幫助全球 17 億無法獲得銀行和金融服務的人，其中，臉書與 WhatsApp、Messenger 融合設計的天秤幣錢包讓用戶可以在線上或離線狀態進行交易無須經過許可，三者的用戶總量高達 27 億人口，即使臉書的計畫是可能實現貨幣全球化的理想計畫，但對政府來說絕不是佳話，各國質疑天秤幣對國家貨幣政策的影響，擔心臉書線上平行貨幣會使中央銀行無法有效控制本國的貨幣供應，在政壇各方的壓力下，天秤幣的發行受到許多阻礙並被推遲到 2021 年（後來改名為 Diem），在新的白皮書當中甚至與諾與各國中央政府合作開發「中央銀行數位貨幣」（central bank digital currency, CBDC）並且併入臉書的網絡當中。[22]

加密貨幣的發展隨著數位金融創新和大型科技公司逐漸進入市場，加速了電子支付發展步伐，更促使國際間興起由央行發行的 CBDC 研發計畫，希望透過央行推行的方式，不僅奠定未來數位交易的基礎，也為回應加密貨幣興起的挑戰。

四、反思:加密貨幣還是貨幣嗎?治理性存在嗎?

本書作者回顧加密貨幣的歷史，這像是一部日漸去中介化的歷史，更貼切法說法是關於去中介化的一波波論述演變過程，加密貨幣提出許多創新的概念為我們的未來譜出截然不同的遊戲規則，加密貨幣從最初的去中心化貨幣到現在蘊含的意涵遠遠不僅於貨幣的概念，他成為投資標的，也成為民眾避險的價值儲藏，其衍生出的金融交易方式對於整個金融體制的變革影響不容小覷。政府與監管機構原先對於加密貨幣認為只是鏈上的貨幣遊戲，但其

[22] Lee Michael，〈重磅！Libra 發布 2.0 白皮書:改發多國「1:1 穩定幣」，還可兼容各國央行 CBDC (臉書幣)〉，《BlockTempo》，2020 年 4 月 17 日，*https://www.blocktempo.com/libra-scales-back-global-currency-ambitions-in-concession-to-regulators/*。

發展至今將構成金融運作的影響，政府欲對加密貨幣加以控制並試圖研發各國央行自行發行的 CBDC 來確保能執行所有金流審查，然而，政府能否迎頭趕上又或是使其現存機制能包容去中心化金融這波來勢洶洶的趨勢？

論及加密貨幣的治理性，有學者就其區塊鏈分叉機制來看，認為區塊鏈本身技術性的硬分岔可能會使加密貨幣使用者內部分成不同陣營，[23]將對治理性造成失誤，[24]然而筆者認為硬分叉本身也是為該類型的加密貨幣做出更具實驗性的淘汰機制，得以隨著使用者體驗篩選出最合適的貨幣，學者討論的治理性若是由政府的角度來看，加密貨幣的演變確實沒有政府置喙的空間，但就該區鏈內部而言，自有其內部可能是中心化也可能是去中心化的自行運行原則，不管如何，以目前的態勢看來其發展有股政府無法抵擋的動力，若持續下去，區塊鏈上的金融服務逐漸得以成熟應用，政府對加密資產的價值流通和許多金融服務的運作都將逐漸失去控制力，那麼加密貨幣是否正在走向實現 20 世紀經濟學家佛烈德利赫·海耶克（Friedrich Hayek）提出的「貨幣去國有化」的路上呢？[25]

責任編輯：李欣樺

[23] 硬分叉往往發生在共識規則的更新，會導致舊有的那些「尚未更新」的節點，不能參與在新的共識機制裡面；而這些沒有更新的鏈，會被保留在單獨原先的鏈上、從此兩條鏈就分道揚鑣，互不幹預彼此的驗證與廣播區塊。硬分叉後的區塊鏈節點是前後不兼容的。

[24] Benjamin D. Trump, Emily Wells, Joshua Trump, Igor Linkov, "Cryptocurrency: governance for what was meant to be ungovernable," *Environment Systems and Decisions*, Vol. 38(2018), pp. 428-429.

[25] Friedrich Hayek 屬奧地利經濟學派，在其 1976 年《貨幣去國有化》的書中，提出允許公民和私人組織等發行自己貨幣的概念，讓他們互相競爭並與政府的法定貨幣一較高下，讓使用人自行決定以哪種貨幣進行交易，根據海耶克的論點，這會導致最適合的幣別勝出，這將會是一種價值不會因政府放任通貨膨脹而產生貶值的貨幣。